Digital and Operational Resilience: A comparative analysis of the EU and UK regulatory framework for the insurance industry from a risk management perspective.

Résilience numérique et opérationnelle : une analyse comparative du cadre réglementaire de l'UE et du Royaume-Uni du point de vue de la gestion des risques.

Stavros Pantos[1]

[1] School of Law, University of Reading, United Kingdom, s.pantos@pgr.reading.ac.uk

RÉSUMÉ. Cet article présente une analyse comparative des exigences de résilience numérique et opérationnelle de l'UE et du Royaume-Uni pour les services financiers. En se concentrant plus particulièrement sur le secteur de l'assurance, compte tenu de son rôle dans la protection contre ces risques, il rend compte des évolutions des pratiques de gestion des risques. Plus précisément, il commente les dispositions prudentielles qui sous-tendent les systèmes, cadres et évaluations de gestion des risques, conformément à Solvabilité II. Le lien entre les activités de risque opérationnel est également abordé dans le prolongement de cette comparaison. Il saisit efficacement comment la reprise après sinistre, la planification de la continuité des activités, la gestion des risques liés aux tiers et l'externalisation se reflètent dans les approches de résilience numérique et opérationnelle. L'objectif de cet article est de mettre en évidence les similitudes et les différences entre les régimes réglementaires de l'Union Européenne et du Royaume-Uni en ce qui concerne les exigences de résilience numérique et opérationnelle des entreprises de réassurance. Des recommandations pratiques pour favoriser le respect de ces deux exigences sous-jacentes sont présentées, aidant ainsi les réassureurs opérant dans ces juridictions.

ABSTRACT. The paper presents a comparative analysis between the EU and the UK digital and operational resilience requirements for financial services. Focusing on the insurance industry, considering its role in providing cover for operational risks, and cyber-related ones in particular, it captures developments in relation to risk management practices. Specifically, commenting on the prudential provisions underpinning risk management systems, frameworks, and assessments, in line with Solvency II. The link between operational risk activities is also discussed as an extension of this comparison. Effectively capturing how disaster recovery (DR), business continuity planning (BCP), third-party risk management (TPRM) and outsourcing are reflected in digital and operational resilience approaches. The purpose of this paper is to highlight the similarities and differences between the EU and the UK regulatory regime in relation to digital and operational resilience requirements for re-insurance undertakings. Practical recommendations to support adherence to both underlying requirements are presented, assisting re-insurers operating in those jurisdictions.

MOTS-CLÉS. gestion des risques, gestion de crise, résilience opérationnelle, reprise après sinistre, planification de la continuité des activités, technologies de l'information et de la communication risques.

KEYWORDS. risk management, crisis management, operational resilience, disaster recovery, business continuity planning, ICT risks.

1. Introduction

Financial resilience has long been the purpose of financial regulation, to ensure market (systemic) stability and customer protection [GOO 98]. Financial stability is considered a key principle of financial regulation [ARM 16], for protection of financial services against prudential risks. The rise of digitalisation of financial services has led to developments to the financial regulatory regime and framework, shifting the focus to operational risks. This contributed to the rise of operational resilience, and digital resilience to an extension, linked to information, communication, and technology (ICT) risks. Operational resilience is considered to be on a par with financial resilience from a risk perspective [NEL 18]. The link between financial and operational resilience is evident when one looks at the approaches to capital management; where capital is required to ensure losses and incidents of

operational risk nature are considered [PRA 24a: par. 3.5]. Operational resilience alongside financial resilience is fundamental in achieving the safety and soundness of the insurance sector [GER 24]. They are the two pillars supporting an insurer's safety and soundness, as well as its adequate customer protection, highlighting the importance of considering financial and operational resilience simultaneously [ABI, 23].

Digital and operational resilience are particularly prevalent in the post Covid-19 world, where operational risks have been exacerbated [BCBS 21a: par. 5-6]. Especially considering cyber risks with their dynamic nature [IAIS 23: par. 6], with digital technologies demonstrating the need for a more comprehensive operational resilience framework to account for the associated operational risks [IAIS 23: par. 4-5]. Digital transformation with cyber security provisions is deemed essential to achieve resilience [SAE 23]. ICT risks are amplified from digitalisation and interconnectedness of the financial sector, with rising cyber risks [EP 22]. Cyber is a key element of operational resilience, with cyber threats allowing financial services to focus on weaknesses and strengths, contributing to a better understanding of their risks [NEL 18]. There are different cyber threats the insurance sector is exposed to, arising from internal and external sources, third parties and outsourcing, with certain activities amplifying these risks [IAIS 16: par. 23]. Cyber risks and their associated responses against them, are an important element of operational resilience [BOE 18]. Operational resilience is interlinked to key regulatory objectives[1] of financial stability, safety and soundness, and customer harm [BOE 18: Fig. 2]. The main supervisory aim is to ensure that in the event of a fail, either financial or operational driven, significant disruption is avoided, and that is orderly [BOE 18: par. 4.21].

Regulatory activity in that space has been intensified at global level, with underlying objective that those risks are understood, mitigated, and controlled, shaping recent policy and supervisory developments [BCBS 21a]. This is particularly interesting for the insurance industry, considering that it provides cover and protection against certain operational risks, such as cyber, and consequently is more exposed to those risks, also from an underwriting perspective. Purchasing insurance is a mechanism to transfer risk and allow for compensation and (partial) recoveries of losses, in the event of an incident happening [COO 15]. There are different insurance policies against certain risks, either single or in aggregate format, mostly for operational risks [PET 11; GAT 14]. Linked to ICT risks, insurance provides protection to minimise losses after a cyber incident (attack and/ or ransomware) outside the risk appetite, with cyber insurance considered a risk transfer mechanism [CRO 23]. Therefore, overall, the role of insurance is essential for the digitalisation and digital transformation, contributing to financial inclusion while helping to build resilience [INS 24b].

Operational performance of re-insurance companies is contingent on the use of technologies and enhanced risk management capacity and capability [ZHA 23]. It is crucial to understand the regulatory requirements underpinning digital and operational resilience of insurers because of the challenges introduced by digital technologies [COS 24]. The increased use of ICT has highlighted the need of operational risk resilience within the re-insurance market [GRI 21]. The impact of digitalisation to the insurance value chain comprises of enhanced customer experience, offering new products, with improved business processes and capacity to prepare for competition with other industries [ELI 18]. This is achieved via the use and application of relevant technologies, in relation to data acquisition and analysis, data storage and communication [ELI 18]. Therefore, the digitalisation of the insurance industry highlights the importance of understanding and managing operational risks.

Moreover, the introduction of fintech and insurtech disrupting the insurance market, with the digitalisation of the insurance value chain, adds another layer of complexity around operational risks and their management, reflected in regulatory developments. The combination of operational risk amplification and regulatory requirement proliferation emphasises the importance of translating the underlying regimes into practice, to support the entities in scope. The digital evolution and use of

[1] Please see Figure 2 of DP01/18, for a graphical depiction of the authorities' supervisory objectives in relation to the operational resilience, in a tiered approach by authority [BOE 18: p. 7].

technologies transforming and revolutionising the traditional insurance business model, underlining the importance of understanding the associated risks [COS 24]. This is particularly the case for financial services institutions, operating in multiple jurisdictions which are often subject to complimentary and/or contradictory regulatory requirements.

The paper starts with a presentation of the two regulatory regimes at EU and UK level, denoted as **"DORA"** and **"OpsRes"** respectively, listing the different publications relevant to re-insurance undertakings. Then, the focus is placed on the risk management provisions of both regulatory frameworks, from a risk management angle. This is segmented into the different components of each regime, capturing risk management practice, systems, and assessments, covering the core elements of prudential nature based on the Solvency II Directive (138/2009/EC) and Delegated Acts (EU/2015/35). An extension of this is the connection with operational risk management, capturing disaster resilience (DR), business continuity planning (BCP), outsourcing with third-party risk management (TPRM). Their relationship with digital and operational resilience is explained in the operational resilience sub-section. Insights on meeting the underpinning prudential provisions are discussed in the penultimate section of this paper, effectively responding to whether the same approach is suitable to meet both regimes. This is expanded before the conclusion, presenting the proposals for a "harmonised" response from re-insurers subject to both requirements with practical recommendations.

2. Methodology

This doctrinal legal research attempts to provides insights on the insurance regulation and supervision in relation to digital and operational resilience requirements. This paper presents a critical analysis of the regulatory regime of digital and operational resilience requirements for certain operational risks. It is focused on describing the regulatory requirements and comparing their associated provisions from a supervisory objective angle. The attention is placed on the UK and the EU regulatory frameworks on the basis that they are leading developments in that area compared to other regulators and supervisors across the world. In the UK regulatory activity has been led by the Bank of England (BoE), the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA), with the European Supervisory Authorities (ESAs) and the European System of Financial Supervision (ESFS) supporting the European Parliament (EP) and the European Council (EC) for the EU regulatory regime. Within this context, the insurance industry is examined, because of its size, significance, and global importance, with Lloyd's of London being the largest insurance marketplace, as most of the largest (and systemically importance) re-insurance undertakings are based in Europe and in the UK. Therefore, the objective of this research is to comment on whether re-insurers subject to both regulatory regimes could meet those requirements with a combined adjusted single approach. Regarding prudential risk management provisions, the underpinning research question considers whether the same practices are sufficient to allow re-insurance undertakings meet both Digital and Operational Resilience requirements. The figure (Figure 1) below depicts the different operational risks considered under those requirements, discussed in the subsequent sections of this paper. It is an expectation that risk management approaches of entities in scope cover all types of risks and their associated activities to identify, monitor, and manage them, with emphasis on operational risks [BOE 18: par. 4.30-4.31].

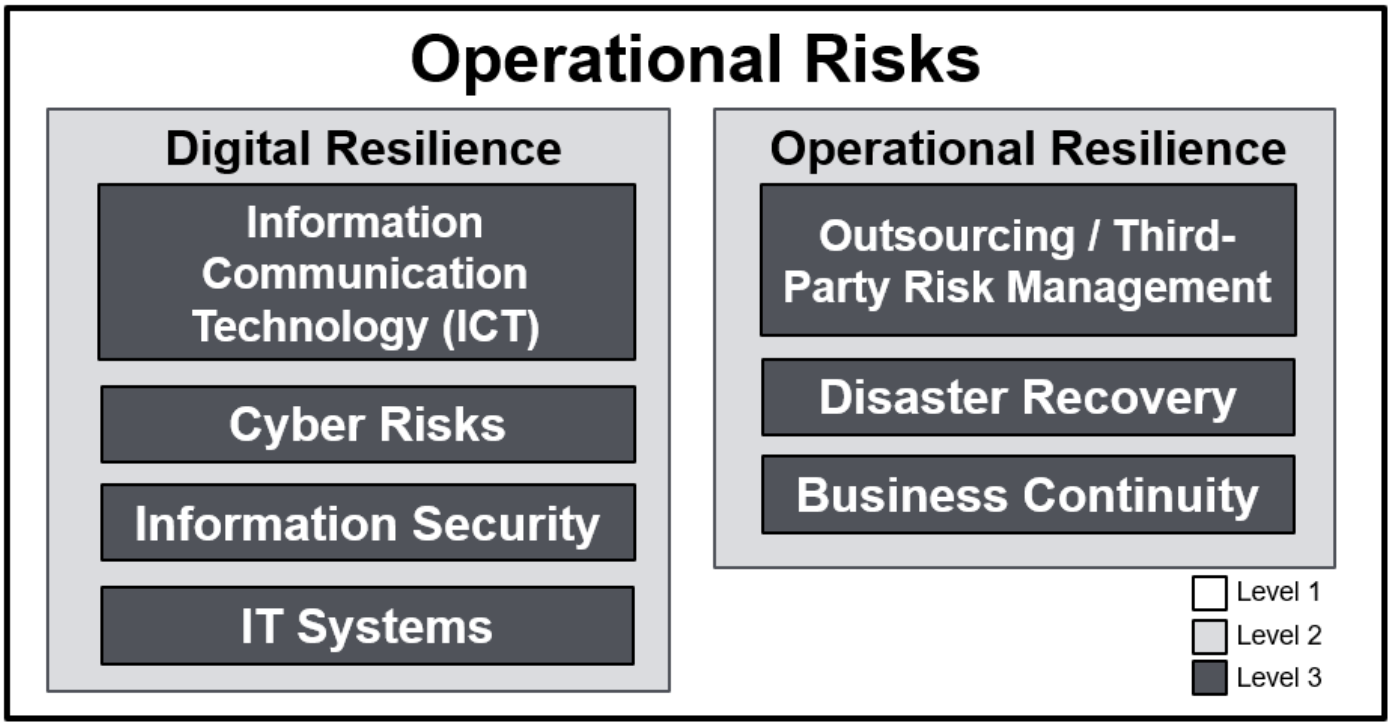

Figure 1. *Operational Risk Universe – Taxonomy*
Source: *own elaboration based on standard risk universe and taxonomy of a re-insurer in line with the Solvency II Standard Formula modules.*

3. Background, Regulatory Regimes and Requirements

The timeline with the key regulatory developments and milestones in relation to digital and operational resilience requirements are discussed in this section. Operational resilience requirements at UK level predate the EU's Digital Operational Resilience Act (2022/2554). From earlier publications in the pre Covid-19 period and during the coronavirus pandemic, the EU DORA Regulation published on 27 December 2022, entered into force on 16 January 2023, and became applicable two years later, on 17 January 2025. The first publication for the UK OpsRes was the joint paper from the Bank of England, the PRA and the FCA in 2018 [BOE 18]. That initial discussion paper focused on operational resilience of the financial system, individual entities, and financial market infrastructures (FMIs) [BOE 18]. Subsequent publications, either joint or individual, followed this, until March 2021, when the 1-year implementation period begun, for firms to operationalise their policy framework [FCA 21a: Fig. 1]. The policy took effect on Thursday 31 March 2022 with the final rules coming into force, when the implementation period ended, with firms required to identify their important business services [BOE 21: par. 4.3, 4.7; FCA 21a: Fig. 1]. Then, the 3-year transitional period commenced, for firms to remain within their impact tolerances (ITols) in relation to the Important Business Services (IBS)[2], ending on 31 March 2025, with a dynamic activity post that deadline anticipated and reflected in the supervisory approach [BOE 21: par. 4.6; FCA 21a: Fig. 1]. By the March 2025 deadline, insurers must had been able to demonstrate that they remain with ITols for all their IBS [GER 24]. For UK insurers, that was a supervisory priority, with the PRA anticipating the management of risks around operational resilience, cyber security and outsourcing pre and post the March 2025 deadline[3] [TRU 25]. Therefore, the phased approach of the UK regulators for OpsRes, with implementation, transition, and business-

[2] In re-insurers, these are typically the departments, functions, areas, supporting the Underwriting and Pricing, Claims, and Complaints Management.
[3] In the LMA's guidance [LMA 21a: p. 4] the timeline graphically depicts the expectations by period (implementation, transition, post-transition), where the Operational Resilience Framework should be fully operational.

as-usual periods, and segmented thematic publications in the 2018-2025 period[4], was a key differentiator compared to the EU DORA.

The dimensions of the UK OpsRes and the EU DORA are captured below. In addition to the legislation and regulatory requirements, publications documenting supervisory expectations from the PRA and the FCA for the UK, and from EIOPA for EU are available. These are complemented from guidance issued by industry bodies, such as the Association of British Insurers (ABI), the Lloyd's Market Association (LMA[5]) for the UK insurance sector[6], and Insurance Europe, for the EU insurance industry. Certain key relevant publications (as of May 2025) are listed in the table below. These are segmented into legislation and regulation, policy and supervision, and industry guidance, split between UK OpsRes vs. EU DORA. This table presents an overview of key documentation capturing the regulatory requirements and supervisory expectations underpinning UK OpsRes and EU DORA, which could be utilised for the regulatory horizon scanning for both entities in scope and not required to adhere to those regimes.

[4] A selection of key UK regulator publications discussed throughout this paper, by year, are the following: 2018 – DP01/18 (BOE, PRA, FCA); 2019 – CP19/32 (FCA); 2021 – responses to CP29/19 and CP19/32 (BOE, PRA, FCA), PS21/3 (FCA), PS6/21 (PRA), PS7/21 (PRA); 2022 – SS1/21 (PRA); 2024 – SoP (PRA), CP17/24 (BOE), PS16/24 and PS24/16 (PRA, FCA).

[5] The LMA represents the 53 MGAs which manage the 84 underwriting syndicates in the market [LMA 20a; b]. The LMA has conducted an Operational Resilience Benchmarking Survey four times, (March 2021, June 2021, September 2021, January 2022) capturing the view from its members [LMA 22a].

[6] Note that additional material with supporting documentation is available from the Cross Market Operational Resilience Group (CMORG) not captured to this table (Table 1).

Publications	UK OpsRes	EU DORA
Legislation & Regulation	–Operational Resilience Instrument 2021, FCA [FCA 21b] PRA Rulebook –Critical Third Party –Insurance Operational Resilience FCA Handbook –SYSC 13 Operational risk: systems and controls for insurers –SYSC 15A Operational resilience –SYSC TP 10 Operational resilience	–Regulation (EU) 2022/2554 [Digital Operational Resilience Act and Delegated Acts] –Regulation (EU) 2024/2956 –Regulation (EU) 2024/1772 [RTS on ICT incidents classification] –Regulation (EU) 2024/1773 [RTS on ICT third-party information] –Regulation (EU) 2024/1774 [RTS on ICT risk management framework]
Policy & Supervision	–D01/18, BoE-PRA-FCA [2018] –CP19/32, FCA [2019] –PS6/21, PRA, [2021] –PS7/21, PRA [2021] –PS21/3, FCA [2021] –SS1/21, PRA [2022] –PRA's Approach to Insurance Supervision, PRA [2023] –Market Operational Resilience Framework, Lloyd's [2023] –SoP: Operational resilience, PRA [2024] –CP17/24, BoE [2024] –PS16/24, BoE [2024] –Operational Resilience Self-Assessments, Lloyd's [2024]	–EIOPA-BoS-24/425, EIOPA [2020] –EIOPA-BoS-20/600, EIOPA [2020] –EIOPA-BoS-20-002, EIOPA [2020] –JC 2023 67, EBA-EIOPA-ESMA [2023] –JC 2023 68, EBA-EIOPA-ESMA [2023] –JC 2023 69, EBA-EIOPA-ESMA [2023] –JC 2023 70, EBA-EIOPA-ESMA [2023] –JC 2023 71, EBA-EIOPA-ESMA [2023] –JC 2023 72, EBA-EIOPA-ESMA [2023] –ESA 2024 35, EBA-EIOPA-ESMA [2024]
Industry Guidance	–IBS Mapping Document, LMA –IBS Selection Criteria and Scoring, LMA [2021] –Indicators of Harm and Intolerable Harm, LMA –LMA response to DP3/22, LMA [2022] –Joint Lloyd's/LMA response to CP29/19, Lloyd's/LMA [2020] –Joint Lloyd's/LMA response to CP19/32, Lloyd's/LMA [2020] –Scenarios and Scenario Testing Industry Guidance, ORCG [2020] –Collaborative Scenario Testing of Third Parties, Effective Practices, CMORG [2024] –Guidance for Firm Operational Resilience, CMORG [2025]	–EXCO-CS-24-012, Insurance Europe [2024]

Table 1. *UK OpsRes and EU DORA List of Key Publications*
Source: *own elaboration, based on publications listed above.*

It should be noted that further guidance is available at global level from the International Association of Insurance Association (IAIS) and from the Basel Committee on Banking Supervision (BCBS) of the Bank for International Settlements (BIS), complementing the above. In particular, the BCBS's Principles for Operational Resilience with the amendments to the management of operational risks, showing the interaction of operational resilience principles with operational risk management, in relation to the risk management environment and activities [BCBS 21a; b]. BCBS defined operational resilience as the ability to deliver critical operations through disruption [BCBS 21a: par. 11]. Despite those BCBS publications focusing on the banking sector, the principles, governance, reporting, and risk management provisions described are equally useful and relevant for the transfer and practical application to the re-insurance industry. These are reflected in the Insurance Core Principles (ICPs) and the common framework of the IAIS; particularly ICP 8 on risk management and internal controls, and ICP 16 on enterprise risk management for solvency purposes [IAIS 24b]. This follows from the IAIS's issue paper in 2023 and the application paper with toolkit for Operational Resilience of 2024 [IAIS 23; IAIS 24a]. Previous work of the IAIS on cyber risks and cybersecurity are partially linked to the operational resilience toolkit [IAIS 16; IAIS 18]. To note that the UK OpsRes policy requirements are aligned with the BCBS consultation on principles of operational resilience [BOE 21: par. 6.1-4]; the prudential angle with the use of scenarios and stress testing to inform operational resilience, and provide assurance regarding resilience, in particular [BOE 21: par. 6.4].

3.1. *UK Operational Resilience*

In the UK, an initial discussion paper (DP01/18, DP18/04) regarding operational resilience of the financial sector was issued jointly by the Bank of England, the PRA and the FCA back in 2018, as the starting point [BOE 18]. Technical innovation, changing behaviours, keeping pace, challenging environment and system complexity are identified as challenges to building operational resilience [BOE 18: Fig. 1]. Preparation, recovery, communications, and governance were noted as core elements for the firms' assessment towards achieving the target level of operational resilience, in line with supervisory expectations [BOE 18: par. 7.4]. The FCA published a consultation paper (CP19/32) the year after in 2019, providing detailed feedback to the initial discussion paper, focusing on impact tolerances (ITols) for important business services (IBS) [FCA 19]. According to the FCA, operational resilience is defined as the

> "ability of firms and FMIs and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions" [BUT 19].

A collaborative response by the Bank of England, the PRA and the FCA was subsequently provided in 2021, covering IBS, ITols and the implementation timeline to deliver operational resilience [BOE 21]. From the FCA perspective, the final rules underpinning UK OpsRes were published in 2021 (PS21/3), commencing the post implementation period [FCA 21a]. The final UK OpsRes rules are captured in the FCA's policy statement PS21/3 [FCA 21a]. Mapping and scenario testing requirements are detailed in the final rules of UK OpsRes [FCA 21a: par. 5.1-18]. The statement of policy underpinning operational resilience was published by the Bank of England in 2021, before being updated in 2024 [BOE 24a;b].

There is a slightly different definition of the IBS between the PRA and the FCA, highlighting the risks and disruption, from a safety, soundness, stability, and customer protection angle, with the PRA emphasising the applicability to Solvency II firms [LMA: 21a, par. 2.2]. This is reflected in their respective requirements, with the PRA and the FCA differentiating their expectations around impact tolerances; though most on the phrasing and framing in supervising the ITols [LMA 21a: par. 4.15-17 FCA, par. 4.18-20 PRA]. Operational resilience requirements for re-insurers with their link to Solvency II are detailed in the supervisory approach of the PRA [PRA 23: par. 97-99]. Operational resilience is a key element of the PRA's Risk Element Framework, and in fact operational resilience

capabilities with areas of vulnerabilities assessed outside ITols are considered a mitigating factor [PRA 23]. Key elements of the UK OpsRes are (i) IBS, (ii) ITols and (iii) the associated testing with mapping [BAI 22]. In the phased approach to identify the IBS, re-insurers in scope could follow certain stages to support the UK OpsRes implementation [CMORG 23] in line with the underpinning regulatory requirements [FCA 21a; PRA, 21a]. The operational resilience stages[7] are (1) information gathering, (2) identifying business services, (3) determining importance, (4) mapping and assigning ownership, and (5) governance and iteration [CMORG 23].

Cyber risk and its management are core components of operational resilience [BOE 18]. Operational resilience, cyber security, and third-party risk are considered key supervisory priorities for insurers in the UK [TRU 25]. From a supervisory perspective, preparation, recovery, communications, and governance are considered key parts of the assessment anticipated for firms and FMIs in scope of the UK OpsRes [BOE 18: par. 7.4]. Policyholder protection is a key supervisory objective from the PRA's perspective regarding OpsRes [BOE 24a: par. 3.38]. In relation to TPRM, the oversight of CTPs with the associated current and emerging risks, support improvements to overall risk management practices [BOE 24a: par. 3.38].

The UK OpsRes requirements and the prudential framework with the overarching supervisory oversight, have been designed in alignment with international reporting frameworks, such as EU's DORA [BOE 24a: par. 1.26]. This underlines that there are common requirements between both regulatory regimes and frameworks, as covered in detail in subsequent sub-sections of this paper.

3.1.1. *Lloyd's of London Principles and Operational Resilience*

A special category of operational resilience requirements at UK level refers to the London market and Lloyd's of London. Lloyd's of London has published different documents, providing guidance and insights to Lloyd's syndicates and managing general agents (MGAs). A key publication from Lloyd's is the Operational Resilience Trends Report, on the back of the Lloyd's self-assessment process, issued in 2022 and in 2024 respectively [LL 24a]. A key part of the UK OpsRes framework is setting the ITols, described by additional data points from insurers' regulatory returns, capturing Policyholder Protection (PP), Intolerable Harm (IH), Firm Safety and Soundness (SS) and Market Financial Stability (FS) [LL 24a: par. 4]. These elements of the UK OpsRes framework are applicable to both Lloyd's syndicates and MGAs[8] [LL 24a]. Testing has been recognised as an area with further improvements, beyond market-wide testing and desktop exercises, with some positive examples from the implementation of testing frameworks developed [LL 24a: par. 7]. Therefore, testing should be expanded to incorporate additional types, such as penetration testing, simulation/ war game, stressed exit for key suppliers, and live systems or operational testing [LL 24a: Table i]. Improvements to the operational resilience scenarios and testing should be accompanied by enhancements to crisis management plans [LL 24a: par. 9]. These should be core components of the testing framework, characterising the scenarios designed from the scenario library, before performing the actual testing [LL 24a: Table j].

Operational resilience is one of the thirteen principles of doing business at Lloyd's [LL 24a; b]. Included as #12 the operational resilience principle states that "managing agents should maintain robust and resilience operations, embedding cyber resilience and effective third-party risk management" [LL 24a: p. 11]. That principle captures the fundamental responsibilities expected from all MGAs in relation to resilience, anticipated by Lloyd's [LL 24]. The operational resilience principle consists of three sub-principles [LL 24a]. These refer to operating a robust operational resilience framework (12.1), maintain oversight of operational resilience through appropriate governance processes and risk and control environments (12.2), and maintaining appropriate cyber resilience (12.3)

[7] For the exact activities and desired output by stage, please see the Operational Resilience Guidance of CMORG [CMORG 23: p. 5-6].

[8] In relation to IBS, 13 factors have been developed to ease their selection, with MGAs being below the required threshold based on size (below the £15bn premium) [LMA 21b].

[LL 24a]. The latter sub-principle (12.3) is divided into seven categories: information systems and reporting (12.3.1), data protection and governance (12.3.2), cyber governance, protection and identification (12.3.3), cyber third-party management (12.3.4), cyber detection (12.3.5), cyber response and recovery (12.3.6), and cyber information sharing (12.3.7) [LL 24a: p. 148-151]. Some of these have been revised[9], with amended wording and merges, in particular about sub-principle 12.3 on cyber resilience, as detailed in the latest Lloyd's principles [LL 24a; b]. For each principle, there are four levels of maturity with differing requirements regarding each sub-principle, segmented in "Foundational", "Intermediate", "Established" and "Advanced" [LL 24a]. There are also connections to other principles, such as principle #10, about governance, risk management and reporting, in relation to the risk and control environment (10.2), and the oversight of operational processes (10.3) [LL 24a; b]. Linked to Lloyd's principles and requirements, scenario testing and mapping of IBS with ITols are areas where further maturity is anticipated in the post implementation period, as reflected in the regulatory guidance [LMA 21a: par. 1.6]. The categories of the operational resilience sub-principles, with linkages to cyber, data, and overall ICT risks (even though these are not explicitly referenced), reveal the similarities to those requirements against those under EU's DORA.

In the UK OpsRes framework, for all re-insurers inclusive of Lloyd's of London syndicates, the central point is the IBS testing against Itols. This is realised via the use of scenarios. Third-party risk management is interlinked to UK OpsRes, especially for re-insurers, recognising their approach to outsourcing, with CTP utilised for strategic activities. An extension of this, similarly not reflected directly in the UK OpsRes regime is about cyber resilience, in managing cyber-related risks, again via scenarios, which are exacerbated by using outsourcing providers in aspects of the digitalised insurance value chain.

3.2. *EU Digital Operational Resilience Act*

DORA aims to strengthen cyber resilience of financial institutions, creating a regulatory framework for ICT risks [CLA 23]. It comprises of developing, maintaining, and adapting the ICT risk management framework based on the overarching digital operational resilience strategy [EP 22: 45]. Certain characteristics have been identified as crucial to determine the effectiveness of digital risk resilience in relation to DORA's requirements [GRI 21]. These are (i) integration, (ii) flexibility, (iii) reliability, (iv) relevance and (v) timeliness, which should describe IT application systems [GRI 21]. DORA's framework dictates the requirements around ICT governance, reporting, and testing, via a risk-based approach, leading to a balanced application of the underpinning requirements [CLA 23].

Chapter II of EU's DORA covers the requirements regarding ICT risk management [EP 22]. As part of DORA, ICT risk requirements are upgraded, and are part of operational risk management [EP 22: 12]. The development of comprehensive capabilities to enable an effective ICT risk management is a core objective of EU's DORA [EP 22: 21]. The dimensions of the comprehensive ICT risk management framework comprise core overarching requirements [EP 22: Art. 6]. Different tools, methods, processes, and policies in managing ICT risks should be part of the framework [EP 22: Art. 15]. Risk management activities shaping the overall risk profile and complexity in relation to ICT are captured in Article 1 of the Delegated Regulation (2024/1774) [EC 24b]. Key elements of these are encryption and cryptography, ICT operations security, network security, ICT project and change management, with data confidentiality, integrity, availability [EC 24b]. ICT security policies, procedures, protocols, and tools are explained in Article 2 [EC 24b]. The risk management framework and systems in meeting the DORA requirements should address the provisions of Articles 2 and 3 of Delegated Regulation (2024/1774) [EC 24b]. In particular Article 3 on ICT risk management, stipulates the different approaches in identifying, treating, and measuring ICT risks [EC 24b]. The ICT risk management requirements are quite comprehensive with further detail in comparison to the UK OpsRes. Article 22 of the Delegated Regulation (2024/1774) on incident management is closer to UK

[9] Please see the latest summary of revisions for 2025 with further detail and the exact amendments to the principles for doing business at Lloyd's [LL 24b: p. 41-49].

OpsRes, linking incidents and their management with ICT risks [EC 24b: Art. 22]. The same applies to Article 24 about business continuity planning and policy [EC 24b]. In fact, the article exhibiting the most similarities with UK OpsRes is the subsequent Article 25, capturing the testing requirements [EC 24b: Art. 25]. Testing of the ICT business continuity is similar to the IBS ITol testing, and the CTP testing, part of the UK OpsRes. In particular the testing of critical and important functions, with scenarios evaluating their ability to withstand disruption and remain operational and functional [EC 24b]. Severe but plausible scenarios should be developed and considered as part of the ICT business continuity plan [EC 24b: Art. 39]. These scenarios are essential component of the testing of business continuity plans [EC 24b: Art. 40]. The ICT risk management framework of Article 27 with reporting requirements is slightly different than the risk management framework under UK OpsRes, where references to a Risk Management Framework (Operational and/ or Enterprise) are included [EC 24b: Art. 27]. Part of the framework is risk appetite, with Article 31 determining the risk tolerance levels and appetite under EU DORA [EC 24b: Art. 31] is similar to the risk appetite and tolerance requirements linked to IBS and ITols of UK OpsRes.

A key component of DORA is the provision of the prudent oversight of critical third-party service providers, establishing a framework for ICT third-party risk management [CLA 23]. The assessment of critical or important operational functions/ activities, under guideline 7, comprises of different factors considered [EIOPA 20: par. 28-9], which have been expanded under DORA's requirements. In the EU DORA requirements, about the management of ICT third-party risks of Chapter V, certain principles are documented for adoption [EP 22: Art. 28], in line with the principles published by the IAIS [IAIS 24a; b] and the EIOPA guidelines [EIOPA 24b]. In Delegated Regulation supplementing DORA, the assessment criteria for an ICT third-party service, whether deemed critical, are captured [EC 24d]. The assessment approach for the criticality of ICT third-party service providers is included in Article 1 of the Delegated Regulation supplementing DORA [EC 24d]. In Delegated Regulation 2024/1773 supplementing DORA, the risk profile of ICT third-party providers is described [EC 24a]. Article 1 presents the characteristics of ICT third-party service providers, explaining how the overall risk profile of the financial entity, re-insurers in this case, are impacted from ICT risks [EC 24a]. The identification and management of risks are supported by the ex-ante risk assessment of critical third-parties of Article 5 [EC 24a]. The risks considered in this assessment are listed, comprising of operational, legal, ICT (plus ICT concentration at entity level) and reputational risks, with risks linked to protection of data confidential or personal), availability of data, data storage, with the location of ICT third-party service provider(s) [EC 24a]. Data templates required for the regulatory returns are explained in the accompanying regulation 2024/2956 [EC 24c]. Article 2 in particular covers the ranking of ICT third-party providers in the supply chain [EC 24c]. In late 2024 before the DORA requirements being applicable, the ESAs performed a "dry-run" exercise to support entities in scope in preparation of the completion of the regulatory returns submission [ESA 24]. Certain lessons learnt with recommendations were also provided, to ease the regulatory reporting [ESA 24: par. 39-57].

Changes to the risk profile from outsourcing arrangements to cloud providers which are critical or important operational functions/ activities, should be considered and reported in the Own Risk and Solvency Assessment (ORSA), according to guideline 2 [EIOPA 20: par. 18-19]. EIOPA drafted 16 guidelines[10] on outsourcing to cloud service providers [EIOPA 20]. Guideline 8 "risk assessment of cloud outsourcing" in particular for ICT risks, is linked to the EU DORA requirements [EIOPA 20]. The focus of risk assessments should be placed on critical or important operational functions and

[10] These 16 guidelines are the following: Cloud services and outsourcing (#1), general principles of governance for cloud outsourcing (#2), update of the outsourcing written policy (#3), written notification to the supervisory authority (#4), documentation requirements (#5), pre-outsourcing analysis (#6), assessment of critical or important operational functions and activities (#7), risk assessment of cloud outsourcing (#8), due diligence on cloud service provider (#9), contractual requirements (#10), access and audit rights (#11), security of data and systems (#12), sub-outsourcing of critical or important operational functions or activities, (#13), monitoring and oversight of cloud outsourcing arrangements (#14), termination rights and exit strategies (#15), and supervision of cloud outsourcing arrangements by supervisory authorities (#16) [EIOPA 20].

activities outsourced [EIOPA 20: p. 9]. This is a common element between EU DORA and UK OpsRes about critical third-parties.

Article 4 of DORA internal governance and control function for the effective and prudent management of ICT risks [CLA 23]. For ICT security and governance, EIOPA devised 25 guidelines[11] [EIOPA 24b]. ICT and security risk management are interlinked, considering the implications of cyber attacks, risk management responses and mitigation, with this relationship reflected in the guidelines combining them [EIOPA 24b: par. 8]. Therefore, ICT and security risks are an integral part of the overall risk management system (guideline 4) [EIOPA 24b: par. 16-8]. Regular testing with assessments and information security reviews links these activities further with the risk management framework (guideline 12), and operational resilience requirements [EIOPA 24b: par. 35-9]. With the testing plan required (guideline 23) [EIOPA 24b: par. 74-77], exhibiting similarities to the UK OpsRes requiring the development, implementation, and application of a testing plan.

Further supplementary Delegated Regulation (2024/1774) accompanying DORA captures the tools, methods, processes, and framework underpinning the management of ICT risks [EC 24b]. The procedures, policies, protocols, and tools linked to ICT risks are essential for their prudent management [EC 24b: par. 10]. In relation to security, these support confidentiality, integrity, and availability of data [EC 24: par. 10]. They also target the identification, evaluation, and management of ICT vulnerabilities [EC 24b: par. 11]. ICT vulnerabilities are key considerations of assessments, and should be central to risk management frameworks [EC 24b: par. 11]. A simplified ICT risk management framework should be introduced [EC 24b: par. 27].

In a similar manner with the UK OpsRes, incidents and their management, in particular associated with cyber threats, are instrumental in the assessments and testing, for the prudent management ICT risks within DORA's requirements [EP 22: Art. 17-8]. Testing for digital operational resilience from Chapter IV of DORA is more comprehensive and detailed compared to UK OpsRes, though serve the same purpose and objective [EP 22: Art. 24]. Testing requirements for digital operational resilience are central to DORA, for the detection of vulnerabilities and the management of ICT risks [EP 22: 25-6]. This approach is similar to the UK OpsRes relying on the application and use of testing as a tool. Developing a testing program with regular testing of operational resilience using vulnerability assessments and threat led penetration tests are core elements of the DORA requirements [CLA 23].

Note that certain insurers who are not in scope of the Solvency II Directive because of their size, are also excluded from the DORA Regulation [EIOPA 24: par. 2.1-2]. EIOPA published an opinion commenting on the reference of the DORA Regulation to Article 4 of the Solvency II directive, about entities excluded from scope [EIOPA 24]. Finally, Insurance Europe provided detailed responses[12] to the draft DORA level 2 measures, with insights against the regulatory technical standards (RTS), draft implementing technical standards (ITS) and draft guidelines (GL) [INS 24a].

ICT risk management is at the core of the EU DORA regulatory framework. The approach in managing those types of operational risks is more holistic compared to UK OpsRes, requiring a framework, systems and their different sub-components (i.e., risk appetite). This is highlighted by the fact that connected risks, such as cyber and information security are part of those provisions.

[11] These 25 guidelines are the following: proportionality (#1), ICT within the system of governance (#2), ICT strategy (#3), ICT and security risks within the risk management system (#4), audit (#5), information security policy and measures (#6), information security function (#7), logical security (#8), physical security (#9), ICT operations security (#10), security monitoring (#11), information security reviews, assessment and testing (#12), information security training and awareness (#13), ICT operations management (#14), ICT incident and problem management (#15), ICT project management (#16), ICT systems acquisition and development (#17), ICT change management (#18), business continuity management (#19), business impact analysis (#20), business continuity planning (#21), response and recovery plans (#22), testing of plans (#23), crisis communications (#24), and outsourcing of ICT services and ICT systems (#25) [EIOPA 24].

[12] Insurance Europe responses to the DORA consultations, providing a view on the guidance and the requirements. Please see the response from Insurance Europe [INS 24a] about the detailed comments.

4. Risk Management Provisions and Practice

In this section, risk management provisions underpinning the UK OpsRes and the EU DORA requirements are discussed further, expanding on their link to operational risk management. These refer to risk systems, risks assessments with testing, and the overarching risk management practice, as well as the connection with other operational risks and associated activities. Risk management should cover all types of risks, inclusive of operational risks, completing their identification, monitoring, and management [BOE 18: par. 4.30]. Operational risk is a risk, whereas operational resilience is an outcome, with this reflected in the approach to management [BUT 19]. Therefore, even though operational risk and operational resilience are different, they are connected. Operational risk management consists of different steps, such as acceptance, mitigation, avoidance [BUT 19], as captured in the Operational Resilience requirements. Consequently the measurement and management of operational risks[13] should be an integral component of the overarching risk management framework [GAT 14]. Operational risks and their quantification are core elements of a holistic Enterprise Risk Management (ERM) approach, towards a comprehensive, integrated, and interdisciplinary risk management framework [MSC 18]. The monitoring and management of operational risk is considered essential for re-insurers [GAT 14]. Operational risk is a key determinant of a re-insurers overall risk profile, impacting its pricing and capital requirements under Solvency II [GAT 14]. It is characterised by past events, but at the same time is unstable, with the capital requirements for operational risk being key for the overall risk management [NAI 19]. For insurers it is of high importance to understand potential risks, and not underestimate their associated costs, based on examples of operational events leading to significant losses [FER 12]. Re-insurance companies have developed operational risk (**"OpRisk"**) frameworks, learning from banking institutions [CRU 15]. The risk and control self-assessment, key risk indicators and loss data (both internal and external) are additional components, supporting the risk measurement and modelling[14], feeding into reporting [GIR 13]. Risk governance and risk appetite are two overarching pillars shaping the Operational Risk Framework [GIR 13]. Risk connectivity[15], with the representation of risks in networks, clusters, and/ or cascades is key to understand operational risks [CHA 19].

4.1. *Operational Risk Activities*

Operational risk management and operational resilience address different goals, but they are interconnected [BCBS 21b: par. 3], explaining why it is important to consider their relationship. The relationship between operational resilience and operational risk management, from a governance and framework perspective, is captured in the IAIS operational resilience toolkit, linked to ICP 7 and 8 respectively [IAIS 24a: par. 16-18]. The BCBS principles for operational resilience are segmented into seven categories: governance, operational risk management, business continuity planning and testing, mapping of interconnections interdependencies of critical operations, third party dependency management, incident management, and resilient information and communication technology, inclusive of cyber risks [BCBS 21a: par. 14]. Principle 2 about operational risk management, is consistent with the IAIS's ICP 8 and ICP 16 about the risk management framework, systems and risk management activities [BCBS 21a]. In relation to stresses, these are flagged under principle 3 about BCP and testing, where a range of severe but plausible scenarios should be examined to evaluate the ability to withstand disruptions [BCBS 21a]. Principle 7 uses the same terminology with EU DORA, commenting on resilience ICT and management of associated risks [BCBS 21a]. The principles for operational resilience of the BCBS are reflected in the revised principles for the sound management of operational risk, focusing on ICT risks [BCBS 21b]. They should become integrated components of the Operational Risk Management Framework (ORMF) [BCBS 21b]. Operational risk management is evolving, with policies, processes/ procedures, and systems of the ORMF required to remain robust to support the adequate management of associated risks [BCBS 21b: par. 13]. The ORMF dimensions are

[13] For perceived problems underpinning operational risk management please see Van Grinsven [VAN 06: Table 4-11].
[14] Different risk assessment tools are presented in Tucker [TUC 15].
[15] Please see Figure 4.2 in Chapelle [CHA 19] for a graphical depiction of a cascade of causes and consequences of operational risks.

expanded in principle 2, about its development, implementation, and maintenance requirements [BCBS 21b]. Part of the ORMF and the ERMF, are risk appetite statements with their associated metrics, indicators, tolerances and capacity, all required under principle 4 [BCBS 21b]. These are linked to the IBS ITols testing when setting risk appetite and the linked key risk indicators evaluated under severe but plausible scenarios. To support both the UK OpsRes and the EU DORA, different operational risk management activities are required. For the effective identification and assessment of associated risks, different tools are available, such as (a) event management, (b) operational risk event data, (c) self-assessments, (d) control monitoring and assurance frameworks, (e) metrics, (f) scenario analysis, with (f) benchmarking and comparative analysis [BCBS 21b: par. 35]. The ICT risk management programme required under principle 10 is aligned to the ORMF [BCBS 21b]. Core components of the ICT risk management are the identification and assessment, mitigation measures and their monitoring with regular tests [BCBS 21b: par. 59]. BCP should also be linked to the ORMF, under principle 11, especially considering the use of scenarios for business impact analysis (BIA), assessments with recovery time objectives (RTO) and recovery point objectives (RPO) [BCBS 21b: par. 63-4].

The UK OpsRes and EU DORA requirements are linked to ICP 8 “risk management and internal controls” [IAIS 24b: p. 74], particularly regarding the systems for risk management and internal controls [IAIS 24b: par. 8.1]. The other ICP linked to the digital and operational resilience requirements is ICP 16 “enterprise risk management for solvency purposes” [IAIS 24b: p. 186]. The UK OpsRes and EU DORA requirements, should be covered under the Enterprise Risk Management Framework (ERMF). This is evidenced from the ERMF components, which are the risk identification, risk measurement (with quantitative techniques), risk appetite, with risk limits and capital adequacy, risk management policies[16], the ORSA and recovery planning [IAIS 24b: par. 16.0.2-4]. Stress testing is part of the ERMF under quantitative techniques to measure risk, for different uses and purposes [IAIS 24b: par. 16.2]. Reverse stress testing and scenario analysis with testing plans for the model and other risk assessments are linked to that [IAIS 24b: par. 16.2.18-24]. In addition to the specific regulatory returns underpinning the UK OpsRes and EU DORA, the risks and output of assessments should be reported in the ORSA. Considering the frequency and nature of these risks, with assessment of current and emerging risks, and their management, with severe but plausible scenarios, digital and operational resilience requirements should be captured [IAIS 24b: par. 16.10-14]. Alignment between reporting requirements underlying EU’s DORA in relation to incident management are noted [BOE 24A: par. 1.26]. Connecting testing and the ERMF is the inter-relationship of the risk appetite, risk limits and capital adequacy, with scenarios used to inform setting risk appetite [IAIS 24b: p. 196-7]. Recovery planning could also be considered an extension of IBS and ITols with their associated testing [IAIS 24b: par. 16.15]. Operational risks are included in the ERMF under Solvency II Directive (article 44) [IAIS 18]. The ORMF and its different components are subject to supervisory review, with the same applied to the operational resilience and operational risk principles respectively [BCBS 21b: par. 69-70]; in the case of re-insurance undertakings could be referenced in the ORSA. In Bailey’s [BAI 22] speech links to certain risk frameworks and tools are presented, mentioning the ORMF and the risk and control self-assessments (RCSAs). Essential elements of operational resilience are risk identification, assessment, mitigation with control implementation, and monitoring [BCBS 21A: par. 7]. These elements support minimising the operational disruptions and associated effects [BCBS 21a: par. 7].

4.1.1. *Business Continuity and Disaster Recovery*

It is important to recognise the interaction of digital and operational resilience requirements with two core operational risks activities: Disaster Recovery (DR) and Business Continuity Management and Planning (BCM/ BCP). BCP is closely linked to operational resilience, with the UK OpsRes requirements contributing to response and recovery capabilities, supporting that relationship [PRA 24a: par. 4.1-2]. BCM similarly should be integrated with risk management frameworks and assessments,

[16] About underwriting, pricing, reserving, investment, liquidity and asset-liability management for instance [IAIS 24b].

via enhanced scope and testing, because of the increased volume and magnitude of operational disruptions [IAIS 23: par. 84-85]. The link of ICT risks with BCM and BCP is highlighted under guidelines 19 and 12 respectively [EIOPA 24b]. DR and BCP are core components of the overall risk management strategy of a company [COO 15]. They are interconnected and part of the business continuity and disaster recovery cycle [TUC 15: Figure 1.1; 1.5]. The DR plan follows the BCP in the business continuity and disaster recovery cycle [TUC 15: Figure 1.1]. Risk assessment and the business impact analysis (BIA) are key steps[17] in the BCP and DR [TUC 15: Figure 1.5]. Disaster Risk Reduction (DRR) is integral to resilience, in building and operationalising it [BOS 14]. An extension of DR is the IT contingency planning (ITCP) to ensure business continuity is achieved [WIB 13]. A risk-based strategy building on synergiesbetween BCP and DR is observed in organisations to meet resiliency requirements [EPS 14]. Linked to that is the Application Impact Analysis (AIA)[18], introduced as a component of continuity management validating the recovery time objective (RTO) [EPS 14]. Robustness and recoverability are two different but interconnected capacities characterising the resilience of financial institutions [BAG 22].

The link between disaster recovery and business continuity has been discussed in the literature. Sahebjamnia et al. [SAH 15] present a framework integrating BCP and DR with strategic, tactical and operational levels, to ensure the efficient and effective resumption and recovery of critical operations after a disruption. Their proposed Integrated Business Continuity and Disaster Recovery Planning (IBCDRP) framework[19] with its different elements and levels, highlights the link between different operational risks, under a hypothetical disruptive event [SAH 15]. The IBCDRP model is expanded in the subsequent work of Sahebjamnia et al. [SAH 18] to account for multiple simultaneous or sequential disruptive incidents. This validates the importance of digital and operational requirements, linking BCP and DR in managing and responding adequately to incidents and operational risk events. The effectiveness of IBCDRP should be evaluated at the three levels of disruption, at minimal, moderate, and major level respectively [DAM 07]. An integrated risk management framework and strategy in relation to business continuity for BCP and BCM, is proposed by Zhing and Zio [ZHI 17]. This integrated risk assessment with different faces linked to businesses processes [ZHI 17] reveals the link between operational risks. The Strategic Business Continuity Management of Niemimaa et al. [NIE 19] comprising of the value preservation (continuity of business model) and value creation (evaluation and modification of business model) parts could be linked to this integrated risk framework[20]. Combining the holistic and strategic approaches to BCM of Niemimaa et al. [NIE 19] support capturing different Operational Risks and their connection within BCP.

4.1.2. *Third-Party Management and Outsourcing*

Resilience is inter-connected with outsourcing and third-party risk management (TPRM). Different types of operational slack and operational scope affect supply chain disruptions at a different extent in the short-term vs. long-term [BAG 22], highlighting the link to outsourcing. Operational risk activities support the detection and prevention of risks leading to operational disruption and incidents [STH 23]. Outsourcing is integral to operational resilience based on the TPRM approaches [PRA 24a: par. 5.1-2]. Rules for critical third-party providers for financial services, are essential for operational resilience, showing the link with outsourcing and TPRM [MIL 24]. ICT third-party service providers support critical and/ or important functions of an insurer, in this case, and this considered a crucial element for the critically assessment and the underlying criteria of the assessment approach [EC 24c: Article 1]. The link between business continuity and contingency planning [BOE 18: par. 4.34-35] with outsourcing for critical service providers has been highlighted in previous UK guidance issued by the Bank of England [BOE 18: par. 4.36-38]. The relationship between operational resilience and

[17] For a graphical depiction of all the business continuity and disaster recovery planning steps in a basic format, please see Figure 1.5 of Tucker [TUC 15].

[18] The AIA cycle is detailed in Epstein and Khan [EPS 14: Figure 1], capturing its different components and risk assessment links.

[19] Please see Figure 2 of the Sahebjamnia et al. [SAH 15] for a graphical depiction of the IBCDRP.

[20] For more detail, please see Figure 1 of Niemimaa et al. [NIE 19] capturing the relationship between value creation vs. value preservation, both parts of the Strategic Business Continuity Management Framework.

operational risk management, with BCP and outsourcing is detailed in the statement of policy part of the UK regulatory environment [BOE 24a]. This is in line with a previous guidance (policy statement PS7/21), where the focus is placed on outsourcing and TPRM [PRA 21b]. This relationship between outsourcing and TPRM with business continuity and exit planning is formalised in the UK guidance [PRA 21b: par. 11.1-17]. Overall, this policy statement (PS7/21) complements operational resilience requirements [PRA 1B]. The equivalent supervisory statement (SS2/21) from the PRA details the provisions around business continuity and exit planning [PRA 24b: par. 10.1-25]. In particular stressed exits are linked to scenario analysis and stress testing, with their results used to inform setting them [PRA 24b: par. 10.10-16]. For a detailed list of the requirements and expectations on outsourcing for insurers please see Table 1 of supervisory statement SS2/21 [PRA 24b: p. 3-4].

4.1.3. *Cyber Risk Management*

Cyber resilience with the management of cyber-related risks is core to operational resilience [FCA 21A: par. 6]. Cyber resilience of insurers is driven by IT transformation and the use of new technologies such as cloud computing [IAIS 23: par. 96]. The IAIS highlights the significance of cyber resilience, IT third-party outsourcing and business continuity with operational risks and their management [IAIS 23: par. 1, 30]. This is explained from the overlapping risks describing those activities, with cyber incidents impacting BCP/ BCM, potentially from an exploited vulnerability at a third-party, thus requiring a broader integrated operational resilience framework [IAIS 23: par. 30]. Digitalisation capabilities drive cyber resilience, utilised in the plan/ prepare and adaptation phases of its process [ANN 21]. In relation to cyber risk management[21], for instance, Eling and Schnell [ELI 16] highlight the importance of developing risk management approaches, especially from the insurance industry, providing data points and information around cyber risks[22]. Cyber risk constitutes one of the most important types of operational risks[23], and thus its management with modelling and quantification should be reflected in the operational risk framework [EGA 19][24]. Digital and operational resilience requirements with the underpinning risk assessment and scenario requirements improve the re-insurers' understanding around cyber risks, and in effect capital management for operational risks [EGA 19]. Therefore, cyber risks and the approach in managing them, using scenarios to understand their nature and loss estimation, should be captured in the internal risk management frameworks [EGA 19]. Cyber risks require an overarching approach to their management part of the risk management framework [ELI 16]. Key aspects of this overarching management of cyber risks are the risk identification, risk analysis, risk management, and risk monitoring [ELI 16]. The challenges of aggregation, distribution, and complex dependencies in relation to cyber risk management and its modelling [ELI 16], underline the need of understanding cyber related risks, with increased data, and also under different scenarios (i.e., cyber-attacks).

Critical third-party (CTP) technology and cyber resilience are connecting operational resilience with cyber-security requirements [BOE 24b]. There are eight different CTP operational risk and resilience requirements [BOE 24b]. These are linked to Governance (#1), Risk management (#2), Dependency and supply chain risk management (#3), Technology and cyber resilience (#4), Change management (#5), Mapping (#6), Incident management (#7) and Termination of services (#8) [BOE 24b]. There is an overlap between CTP operational risk and resilience requirements, in relation to risk management

[21] The four pillars of cyber risk management according to the CRO Forum [CRO 14] are (i) preparation, (ii) protection, (iii) detection and (iv) improvement.

[22] The common classification and codification of cyber risk, understanding of cyber risk exposure accumulation, with a strong and well designed risk management framework, are the core three elements required to support the insurance market for cyber risks and associated assessment [CRO 14].

[23] Insufficient or poor quality loss information, with uncertain value, highly interconnected IT systems, and continually evolving attack strategies, perpetrators and motives are challenges characterising the insurance market of cyber, from a risk management perspective [CRO 14: p. 20].

[24] Different cyber related risks scenarios are described and examined in the publication of Egan et al. [EGA 19], derived from a working party publication of the UK Institute and Faculty of Actuaries, detailing real scenarios with implications in monetary terms based on the UK insurance industry.

[BOE 24b]. The use of scenario testing is connecting operational risk management and operational resilience with CTP oversight [BOE 24b]. The second requirement underpinning CTP operational risk and resilience is risk management [BOE 24b]; this connects CTP technology and cyber resilience [BOE 24b]. According to that requirement re-insurers in scope need to develop capabilities to identify, assess, and remediate vulnerabilities linked to information and technology [BOE 24b: par. 2.21]. This exhibits similarities with the EU DORA in relation to ICT risks, with the scenarios and the incident management playbook in particular [BOE 24b: par. 2.155-7]. Cybersecurity of insurers is part of the supervisory review and assessment captured in the ORSA [IAIS 16: p. 31]. According to the IAIS, best practices for cyber resilience in relation to the cyber resilience programme and risk management framework, include governance, identification, protection, detection, response and recovery, testing, situational awareness, learning and evolving [IAIS 16: par. 38-9]. Moreover, there are different standards around cyber security, in relation to frameworks and guidance, such as the G7 Fundamental Element of Cyber Security for the Financial Sector (G7FE), the G7 Fundamental Elements for Effective Assessment of Cybersecurity for the Financial Sector (G7FEA), and the CPMI-IOSCO guidance on cyber resilience for financial market infrastructure [IAIS 18: par. 8].

Overall, it is highlighted that digital and operational resilience requirements should be regarded as part of operational risk management activities. There are three distinct areas of operational risk management interlinked with the digital and operational resilience, as covered in the requirements – either directly or indirectly; these are business continuity with disaster recovery, third-party management and outsourcing, and finally cyber resilience, connecting the other two categories with the management of cyber risks. This relationship between the different types of operational risk management activities is observed in global guidelines and principles for re-insurance undertakings (i.e., IAIS ICPs), transposed at local level for the UK OpsRes and the EU DORA regimes.

4.2. *Testing and Scenarios*

The use of stress testing in the risk-based prudential supervision has been intensified since the global financial crises, initially for banks, and then for insurers [ARM 16]. Scenario analysis is a core element of the Operational Risk Framework[25] [GIR 13]. The use of scenarios in measuring operational risk capital has been discussed in the literature, commenting on the calibration of loss-generating and risk modelling [DUT 14]. It is possible to calculate the required operational capital under Solvency II for re-insurance undertakings using scenario analysis [VYS 20]. Despite the fact that there is no specific capital requirement linked to operational resilience, it is expected that firms hold enough capital to absorb losses arising from operational risks and incidents linked to operational resilience [BOE 24b: par. 3.5]. Scenarios are referenced in the operational resilience requirements as a key tool utilised. The examination of scenarios under the DORA and the UK OpsRes requirements could support the quantification of re-insurers' capital for operational risk, in line with the Solvency II Solvency Capital Requirement (SCR) [PET 11]. Scenario testing with impact tolerances supports the establishment of a proportionate operational resilience [BOE 18: par. 5.5, Fig. 5]. To understand the importance of the use of scenarios and testing, certain fundamental principles have been developed for UK OpsRes, to ensure consistency and improvements in applications and practices [CMORG 23]. These seven principles[26] [CMORG 23: par. 5.1.3] could also be considered for the DORA testing requirements.

4.2.1. *Testing Plan*

Severe but plausible scenarios are required for operational resilience testing [PRA 22: par. 6.2]. These scenarios should be detailed in the testing plan, providing assurance that the IBS evaluated remain within ITols [PRA 22: par. 6.6]. The importance of developing a testing plan is highlighted, with a testing schedule, and a range of scenarios within and exceeding ITols [LMA, 21a: par. 5.3-5].

[25] The Operational Risk Framework is described in Girling [GIR 13: Figure 3.1].

[26] Please see the CMORG guidance detailing those 7 principles of scenarios and the development of the testing plan [CMORG 23: p. 30-31].

The development of a testing plan is a key requirement of the UK OpsRes framework under scenarios and their assessment. To support the development of a scenario testing plan, the scope, priorities, frequency, and risks impacted, are core components that should be detailed [ORCG 20; CMORG 23: par. 5.1.2]. The testing plan for UK OpsRes is linked to the Stress and Scenario Testing Framework (SSTF) developed by re-insurance undertakings as part of the ORSA process, as anticipated based on the Solvency II requirements [PRA 23: par. 84]. Scenario tests should be embedded into existing frameworks and approaches about setting risk appetite, capturing the impact and likelihood, using risk materiality matrices [PRA 24a: par. 3.4]. Approaches to testing are linked to existing risk management requirements, linking operational risk testing [PRA 21A: par. 7.12-15]. Linking the UK OpsRes requirements with other operational risks, scenario testing should be used as an assessment for outsourcing and TPRM [PRA 21a: par. 7.6-11]. This is because third-parties and supply chain implications are considered in the testing requirements [FCA 21a]. The scenario consideration for CTP capture continuity of service provisions, failure or disruption of 'internal essential services', stressed exit of a key provider, as well as climate related events [BOE 24b: par. 2.155].

4.2.2. *Characteristics and Requirements*

Scenario testing requirements under UK OpsRes are detailed in supervisory statement SS1/21 [PRA 22: par. 6.1-13]. Severe but plausible scenarios should be examined, with realistic assumptions, in line with the testing plan [PRA 22: par. 6.2]. These severe but plausible scenarios should support the identification of further IBS(dynamic in the nature of the threat), capturing single or multiple IBSs, with dynamic severity [LMA 21a: par. 5.3]. Scenario tests with their assumptions and results, management actions to address, mitigate or risk accept the output, and the underlying lessons learned, are core to the self-assessment exercise and documentation [LMA 21a: par. 5.8]. The ORCG highlights in its guidance five proposed stages to scenario testing, reflecting those characteristics: (1) define the scenario; (2) gather information; (3) test ability to remain within ITOls; (4) define improvement options; (5) document test outcomes [ORCG 20: p. 11]. The type of scenarios (i.e., desk-top exercise, simulation etc.), their frequency, number of IBS tested, availability and integrity of resources, with the environment in a dynamic set-up conditional on vulnerabilities, are factors to consider when developing the testing plan, and key elements of the scenario requirements [PRA 22: par. 6.6]. Additional scenario and testing requirements are captured in the PRA's guidance (SS1/21), explaining the supervisory expectations in relation to testing [PRA 22: par. 6.1-13]. The timeline and magnitude of service disruption/ resumption, determined by the stress severity, are key characteristics of the scenarios [ORCG 20]. Another important angle of the operational resilience scenarios is the ability to understand their circumstances, with the identification, management, monitoring, and reporting of associated risks [PRA 23: par. 66]. Other characteristics are the cost of running the tests and the underpinning incident data used in those exercises [PRA 21a: par. 7.1-20]. In evaluating the scenarios for IBS, the ORCG highlights five pillars to consider; people, facilities, technology, information, and third party, about the disruption and loss [ORCG 20: p. 20].

Scenario analysis is considered of high importance, on the basis that it introduces proportionality [BOE 18: par. 5.5]. In particular when combined with the ITol assessment, since scenarios are used to establish a proportionate level of operational resilience, indicating whether disruption leads to recovery within or outside tolerance, based on severity [BOE 18: par. 5.8-5.9]. Butler [BUT 19] initially highlighted the purpose and requirements of testing underpinning operational resilience, to support firms evaluate their ability to withstand a severe event with reference to the IToLs and IBS, and effectively the outcome of testing utilised to identify resilience gaps. ITols, as a core element of UK OpsRes, are associated with the risk appetite[27] [PRA 24a]. After setting ITOls for disruption to critical services (ICPs 8 and 16), testing with the use of scenarios is required [IAIS 24a: p. 8] according to the UK OpsRes requirements. Testing with self-assessments supports improvements to operational resilience practices and frameworks, in line with ICPs 8 and 16 [IAIS 24: p. 8]. Testing ITols under

[27] In the Operational Resilience Statement of Policy, the relationship between risk appetite and importance tolerance is explained [PRA 24a: Fig. 2].

extreme but plausible scenarios is considered a key requirement [MIL 24]. Extending that, response plans should be available post testing, evidencing robust capabilities, and plans for strategic investments to ensure improvements [MIL 24]. This is required because of the anticipated maturity of scenario testing, with depth and consistency of approach and design, clarifying the (i) cause of the disruption, (ii) the scale of the disruption and the (iii) key risk factors and vulnerabilities subject to testing [MIL 24].

4.2.3. *Identification and Examples*

For the identification of different severe but plausible scenarios, internal and external resources could be explored. Internal resources are derived from risk registers, past risk events and incidents, plus other scenarios from regulatory reporting (i.e., ORSA, capital model), with regulatory publications and examples from research institutes and governmental bodies considered as external sources[28] for input [ORCG 20: p. 9; CMORG 23: p. 31]. Industry-wide tests are examples of additional scenarios[29] which could be considered to meet the testing requirements [FCA 21a]. Further examples of IBS scenario tests are detailed in the guidance of the Cross Market Operational Resilience Group [CMORG 23]. These are workspace unavailability, loss of IT service, loss of data centre, disruption of critical supplier, cyber event DDoS, critical market infrastructure unavailability, cyber event critical data compromise, and widespread cyber event impacting data and infrastructure [CMORG 23: par. 5.1.1]. For the available testing types, these range from a simulation/ war game, a tabletop/ desktop exercise, a structured scenario exercise (SSE), a drill, live systems or operational testing, and operational incidents, according to the examples from the ORCG guidance [ORCG 20: p. 14]. Further improvements are anticipated around cyber stress tests, in relation to cyber and digital resilience, as part of the overarching macroprudential oversight of operational resilience [STH 23].

The use of scenarios is a core characteristic both the UK OpsRes and the EU DORA regimes have in common. The application of this tool for testing is essential, to identify vulnerabilities, confirm "resilience" in line with the risk appetite set, and support the development of applicable management actions and mitigating strategies. The scenario characteristics and testing requirements are detailed in the plan, explaining why, when, what, and how tests are performed effectively. Considering the importance of testing, examples of scenarios are provided from regulatory prescribed stress tests and in guidance published by regulators and industry bodies. These externally provided scenarios are useful benchmarks. They could be utilised for both the actual testing, as a point of reference, and also to support improvements to risk practice (i.e., assessments, modelling, quantification).

5. Discussion

Despite differences in the detailed requirements of both regimes, the ultimate objective and scope in managing those operational risks towards resilience remain the same. The overarching principles of IAIS (ICPs) compose a common foundation observed in both regulatory frameworks. By design there is an alignment between UK's and EU's approach in managing digital and operational resilience. EU DORA's requirements are more detailed and at the same time broader than UK OpsRes. The UK requirements are documented in a collection of policies and supervisory guidance, whereas EU DORA comprises of the detailed regulation with the accompanying delegated regulations and provisions. In the UK industry bodies and consortiums have published guidance for re-insurers in scope, with practical applications and examples, complementing the regime. This approach is not observed in Europe, with EIOPA only publishing guidelines for re-insurance undertakings. In relation to the scope, cyber resilience with cyber risks, and cyber security are captured under DORA. However, they are not

[28] A selection of them is included in the ORCG guidance, such as the National Risk Register (NRR), the Global Risk Register (GRRC), the Business Continuity Institute, the ORX incident database, the National Cyber Security Centre, the World Economic Forum (WEF), and the Cyber Security Information Sharing Partnership (CSIP) [ORCG 20: p. 4].

[29] For actual scenario examples with detailed impact, split into the themes of date, technology, third-party, facilities & people, please see the scenario library of the ORCG [ORCG 20: p. 21-25].

explicitly considered under the OpsRes in the UK, linked indirectly based on further requirements from the BoE, the PRA and the FCA for UK re-insurers. Operational resilience, cyber security, and third-party risk are considered key supervisory priorities for insurers in the UK [TRU 25]. Moreover, differences in the terminology used between the two regimes are highlighted. For instance, IBS and ITols are key words for the UK OpsRes, but not used in EU DORA. Equally, ICT risks are central to DORA, but not referenced widely within UK OpsRes. The use of severe but plausible scenarios, with detailed testing, are common elements of both regimes. The same applies to certain risk management activities, such as the identification, monitoring, management, and reporting of associated (operational) risks. However, under EU DORA new risk management practices are required, tailored to ICT risks, with the development of the ICT Risk Framework. Extensions to existing risk management practices are mentioned under both UK and EU requirements, though DORA's expectation are wider, and towards new frameworks. From the recommendations as in table above, a hybrid approach is proposed to achieve meeting both requirements, effectively with adjustments to the ERMF and ORMF, based on the digital and operational resilience, with the addition of the ICT Risk Framework. This is partially reflected in the reporting requirements. Under both regimes specific regulatory returns are required, although the requirements under DORA are more granular. From a prudential angle and Pillar II of Solvency II, key risk activities in meeting both requirements should be included in the ORSA process, and documented in the ORSA Report. Finally, in relation to their application, about the entities in scope, a simplified approach about the framework for ICT risks is prescribed in DORA, for a proportionate and pragmatic approach. For the UK OpsRes the expectations are uniform, with variations in terms of maturity, based on materiality. To note the limitation about the entities outside Solvency II, with a pragmatic approach proposed for the non-Directive firms. Even if they are not in scope, the digital and operational resilience requirements, and in particular testing with the management of risks, could support those entities improve their internal approaches.

6. Practical Applications and Recommendations

After discussing the relationship between digital and operational resilience with operational risk management activities, the question remains on how best to approach meeting simultaneously both requirements. The answer is that by adopting the principles underpinning those two regimes, and improving approaches to risk management, re-insurance undertakings in scope could cover both requirements simultaneously. Practical applications and considerations for re-insurance undertakings in scope of both the UK OpsRes and the EU DORA are captured in the table (Table 2) below. These practical recommendations for Digital and Operational Resilience are codified by risk management provision, into risk activities, the risk framework, appetite and testing, ending with the risk assessment. Requirements introduced by both regimes should be integrated into existing practices, unless the introduction of new approaches are stipulated, as for the ICT Risk Framework for instance.

Risk Management Provisions	Digital and Operational Resilience
Risk Activities	–Business Continuity Management and Planning –Disaster Recovery –Outsourcing and Third-Party Risk Management –Cyber and Cyber-Security Risks –Identification of Important Business Service and Critical Third Parties
Risk Framework	–Extensions to the ERMF for OpsRes Framework –Adjustments to the ORMF for OpsRes Framework –Establishment of the ICT Risk Framework –Links of ICT Risk Framework with ORMF –Amendments to existing policies, processes, and procedure documents –Creation of ICT risk activity tailored protocols and policies –Updates to control environment for mitigation of new and existing risks –Advances to approach in managing incidents, loss and risk events
Risk Appetite	–Use of severe but plausible scenarios to inform setting it –Tolerance built-in (ITol) based on type, frequency, severity of incident and level of disruption –Risk-specific appetite by type of risks (for each ICT) –Risk activity-based assessments validating appropriateness of tolerances
Testing	–Horizon scanning and benchmarking for scenarios from external sources –Development of list of severe but plausible scenarios for resilience –Creation of a testing plan –Testing with scenarios for BCP/ BCM, DR, TPRM, Cyber Risk/ Security based on scenario playbooks and testing guidance –Documentation of testing results with updates to Framework -Utilising regulatory prescribed stress tests as benchmarks
Risk Assessment	–Assessments based on risk activities, documented in their processes –Regime specific regulatory returns and data/ template submissions –Disclosures and reporting in the ORSA process and report –References in the Solvency & Financial Conditions (SFCR) report

Table 2. *Risk Management Practical Approaches & Recommendations for Digital and Operational Resilience*
Source: *own elaboration from recommendations discussed above.*

It is assumed that enhancements to risk management practices in relation to the risks, and risk activities in scope of both regimes, are deemed sufficient in supporting re-insurance undertakings to ensure adherence. While entities in scope cannot avoid having the two separate regulatory returns and meeting specific UK OpsRes and EU DORA requirements, by strengthening their risk management practices and systems, will allow them to understand and manage those operational risks, instrumental for both regimes. In addition to the developments in those different areas of risk management provisions, a gap analysis and maturity assessment should also be performed by the entities in scope. The gap analysis, looking at the UK OpsRes and the EU DORA requirements, aims to showcase the internal weaknesses and the pathway to improvements; beyond minimum regulatory adherence. This is validated by the maturity assessment, reading across from the gap analysis results and synthesizing towards creating the

target operating model for risk management in line with digital and operational resilience requirements. The recommended combination of the gap analysis with the maturity assessment against risk management provisions (as in the five categories from Table 2 above) aims to support the advances and developments to meet digital and operational resilience requirements.

Advances to risk management practices, the risk frameworks, risk systems, and overall risk activities capturing those operational risks, inclusive of ICT, could lead to improvements and regulatory compliance. This is graphically depicted in the integrated digital and operational resilience risk management. Risk management for digital and operational resilience is captured in the figure (Figure 2) below. The starting point is the risk management framework, with the ORMF which includes OpsRes and the ICT Risk Framework. These frameworks are developed based on the ERMF, and effectively are attached to it as an extension focusing on the Operational and ICT risks respectively. Components of this, based on risk management systems and programs, are the associated policies, processes, procedures, protocols, and controls from the control environment. These policies, processes, procedures, protocols, and controls are tailored to digital and operational resilience, capturing specific activities and risks. For instance, the approach to testing with the detailed characteristics of scenarios could be explained in a procedure document, used by the business in performing those tests. The same applies to the controls based on resilience activities, reflected in the relevant risk registers. There is an interaction between risk management practice, in relation to the rest operational risk activities, linking them with operational and digital resilience. This refers to business continuity, disaster recovery, outsourcing and cyber risk management, as explained in previous section. These operational risk activities are integrated to digital and operational resilience. They contribute to the management of the associated operational risks, revealing their interconnectedness and correlation with the underlying risk drivers (i.e., how the risk of default of the critical outsourcing provider, that is part of the BCP should be tested under scenarios for digital and operational resilience). These activities support the identification of vulnerabilities throughout the insurance value chain, allowing re-insurers design effective mitigation techniques, and enhancing holistically their control environment (e.g., critical claims data used for underwriting decisions stored in cloud-based backups). There is overlap between those activities, that is why it is important to highlight their interconnection, since if all these are executed as per internal plans, it would make the approach towards digital and operational resilience more robust. Plus, certain requirements are probably already met as part of those activities (i.e., assessing CTPs). The outcome of those risk management activities is used to inform the risk appetite and its characteristics, such as the statements, tolerance, capacity, limits, and metrics, with the key risk indicators (KRIs). There are existing risk appetite statements and metrics attached to each risk activity, thus certain of them could be refined to complement the ones introduced to address fully the digital and operational resilience requirements. These consequently are evaluated via testing, with the obtained results confirming the appropriateness and validating their exact dimensions (i.e., soundness of metrics, exact triggers and limits). All these core components of risk assessments are part of the regulatory submissions, with specific returns based on the UK OpsRes and EU DORA. It is anticipated that these results are evaluated as part of the supervisory review, and thus are documented in the Solvency II ORSA process and report. Specifically, it is suggested that a summary of those activities is included in the ORSA, with the emphasis placed on the risk quantification, explaining the stress and scenario tests, their obtained results and changes to risk appetite and strategy conditional on their output. These elements of digital and operational resilience with their interconnection within operational risk management are graphically depicted in the following figure (Figure 2).

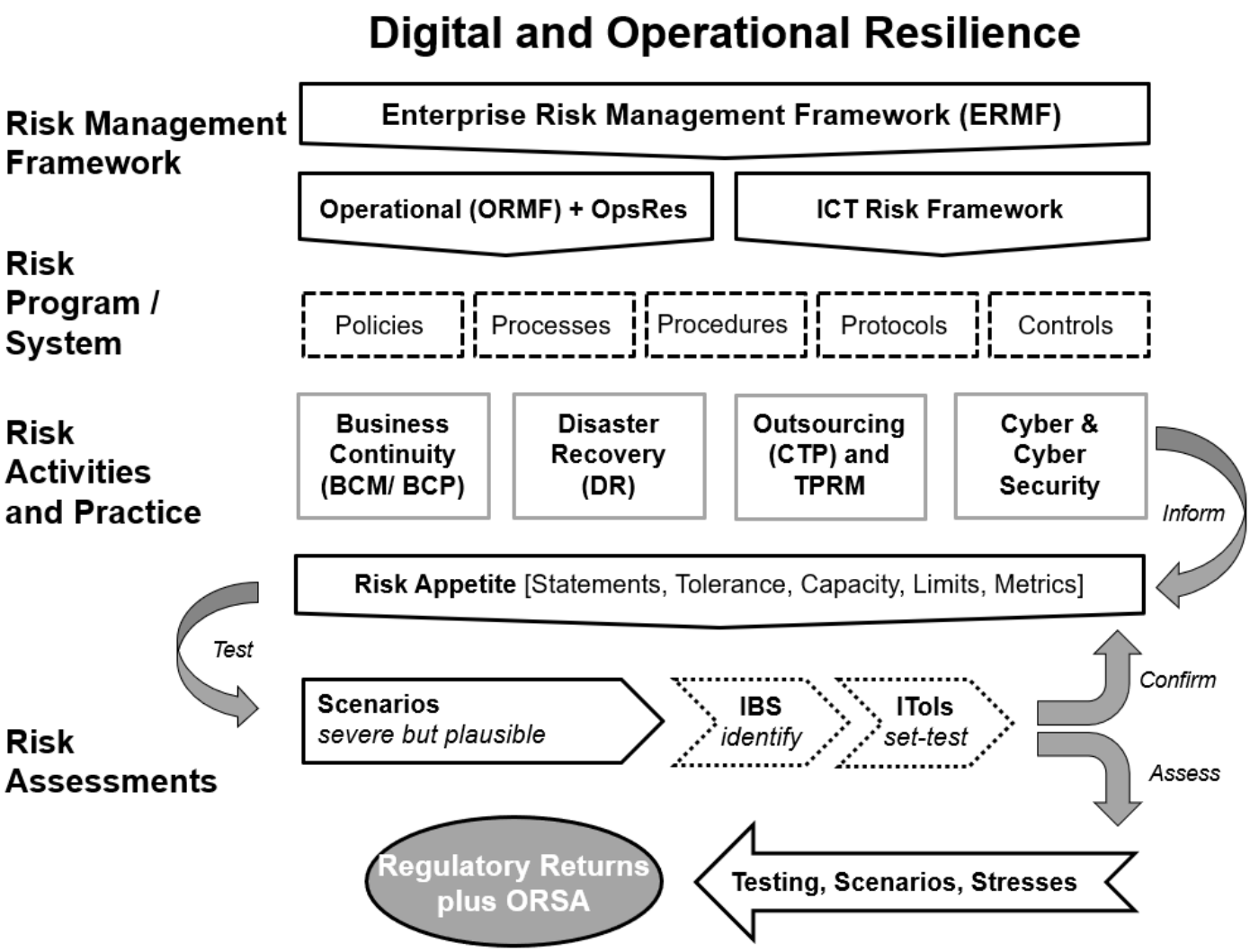

Figure 2. *Digital and Operational Resilience Risk Management*

Source: *own elaboration based on UK OpsRes and EU DORA regulatory regimes and requirements.*

The requirements of digital and operational resilience regimes re-shape the operational risk management. Re-insurers in scope of both regimes should integrate these requirements into existing frameworks, systems, and risk activities. To support regulatory compliance with those regimes adjusted scope of risk management practice is needed. The emphasis should be placed on understanding the nature of the risks central to digital and operational resilience. This refers to mapping them against existing risks, revealing their associated risk drivers, and untangling how these cascade into the business from core insurance activities and operations. The identification of those operational risks is an essential element of their management, and that is because it is important to realise the connection between TPRM, DR, BCP and cyber risk management, and how these are interlinked with digital and operational resilience. The interplay between existing operational risk activities should be clarified in the frameworks, policies, processes, and all relevant internal documentation. This allows the business to gain an increased understanding of the risks, the activities to manage them, and overall, how to prepare with the controls and mitigants. It also contributes to the robustness of those activities, having a holistic approach to manage those operational risks and their sub-categories towards resilience. The ultimate objective of digital and operational resilience is the same, the angle varies, and this is explained at each activity level. In practice re-insurers in scope of both regimes could achieve regulatory adherence by improving existing operational risk management activities to (i) capture the risks not considered already (i.e., ICT) and (ii) create targeted approaches based on the requirements (e.g., testing ITols of IBS using scenarios).

7. Conclusion

This paper highlights the links of digital and operational resilience with operational risk management. Analysing the UK and EU regulatory framework, the focus is placed financial services, and in particular on re-insurance undertakings, to understand the resilience requirements. The risk management provisions of the UK OpsRes and the EU DORA requirements are discussed, commenting on the risk activities and testing. In particular about DR, BCM/BCP and outsourcing with TPRM and cyber risks, and their relationship within digital and operational resilience requirements.

In summary, this paper adds to the operational risk management literature, after highlighting the links between digital and operational resilience with operational risk management activities. It provides a comparison of the UK OpsRes vs. the EU DORA regulatory framework about operational resilience, focusing on certain components of both regimes in relation to the management of operational risks, emphasising on scenarios and testing (section 4). The key publications with the regulatory requirements, supervisory expectations and industry guidance underpinning those regimes are listed (Table 1) and explained (section 3). Proposals for risk management developments and advances in meeting both regimes simultaneously are discussed following from the comparative analysis between those two regulatory frameworks are covered. Finally, practical recommendations for risk management professionals of re-insurers are discussed (Table 2, Figure 2), with advice for improvements and enhancements to operational risk management practice. A limitation of this study to note is the empirical component, since data from the digital and operational resilience reporting could enrich this comparison. An empirical assessment of both regulatory regimes could extend this research further, commenting on their actual effectiveness based on disclosures from re-insurers in scope. This involves looking at the SFCR and annual reports with accounts, capturing the information presented about operational risk management. Even though detailed disclosures based on the exact requirements such as the identified IBS and ITols are not publicly available, the tone and commentary from those reports could reveal the level of embeddedness, deepening the critique between the digital and operational resilience regimes.

Bibliography

[ABI 23] ABI, “The Two Pillars – Financial and Operational Resilience”, Tuesday 21st November 2023, the Association of British Insurers, 2023.

[ANN 21] ANNARELLI, A., PALOMBI, G., “Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework”, *Sustainability*, 13, 13065, 2021. https://doi.org/10.3390/su132313065

[ARM 16] ARMOUR, J., AWREY, D., DAVIES, P., ENRIQUES, L., GORDON, J.N., MAYER, C., PAYNE, J., *Principles of Financial Regulation*. Oxford University Press, Oxford, 2016.

[BAG 22] BAGHERSAD, M., ZOBEL, C.W., “Organizational Resilience to Disruption Risks: Developing Metrics and Testing Effectiveness of Operational Strategies”, *Risk Analysis*, Vol. 42, No. 3, p. 561-579, 2022. DOI: 10.1111/risa.13769

[BAI 22] BAILEY, D., “Operational resilience - next steps on the Prudential Regulation Authority‘s supervisory roadmap”, Speech (virtual) by Mr David Bailey, Executive Director for International Banks Supervision of the Bank of England, at the UK Finance Webinar “Operational Resilience: Beyond", 28 April 2022, Bank of England, 2022.

[BCBS 21a] BCBS, “Principles for Operational Resilience”, Basel Committee on Banking Supervision, March 2021, Bank for International Settlements, 2021.

[BCBS 21b] BCBS, “Revisions to the Principles for the Sound Management of Operational Risk”, Basel Committee on Banking Supervision, March 2021, Bank for International Settlements, 2021.

[BOE 18] BANK OF ENGLAND, “Building the UK financial sector’s operational resilience”, July 2018, Discussion Paper, Bank of England DP01/18, PRA DP01/18, FCA DP18/04, Bank of England, 2018.

[BOE 21] BANK OF ENGLAND, “Operational resilience: Impact tolerances for important business services”, March 2021, Responses to Bank CPs relating to FMIs, Responses to CP29/19, Responses to CP19/32, Bank of England, 2021.

[BOE 24a] BANK OF ENGLAND, "Operational resilience: Operational incident and outsourcing and third-party reporting", 13 December 2024, Consultation Paper CP17/24, Bank of England, 2024A.

[BOE 24b] BANK OF ENGLAND, "Operational resilience: Operational incident and outsourcing and third-party reporting", 12 November 2024, PS16/24, PRA policy statement 16/24, FCA policy statement 24/16, Bank of England, 2024.

[BOE 25a] BANK OF ENGLAND, "Operational resilience of the financial sector", Bank of England, 2025. https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector

[BOE 25b] BANK OF ENGLAND, "Operational Resilience: Policies relating to operational resilience for Solvency II insurers", Bank of England, 2025. https://www.bankofengland.co.uk/prudential-regulation/prudential-and-resolution-policy-index/insurance/operational-resilience

[BOS 14] BOSHER, L., "Built-in resilience through disaster risk reduction: operational issues", *Building Research & Information*, 42 (2), p. 240-254, 2014. https://doi.org/10.1080/09613218.2014.858203

[BUT 19] BUTLER, M., "The view from the regulator on Operational Resilience", Speech by Megan Butler, Executive Director of Supervision: Investment, Wholesale and Specialist, delivered at TISA's Operational Resilience Forum, London, Financial Conduct Authority, 2019.

[CHA 19] CHAPELLE, A., *Operational Risk Management: Best Practices in the Financial Services Industry*, John Wiley & Sons, Chichester, West Sussex, 2019.

[CLA 23] CLAUSMEIER, D., "Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)", *International Cybersecurity Law Review*, Volume 4, p. 79-90, 2023. https://doi.org/10.1365/s43439-022-00076-5

[CMORG 23] CMORG, "Guidance for Firm Operational Resilience", Version 2, November 2023, TLP CLEAR, Operational Resilience Collaboration Group (ORCG), 2023.

[COO 15] COOK, J., "A Six-Stage Business Continuity and Disaster Recovery Planning Cycle", *S.A.M. Advanced Management Journal*, Vol. 80, No. 3, p. 23-33, 2015.

[COS 24] COSMA, S., RIMO, G., "Redefining insurance through technology: Achievements and perspectives in Insurtech", *Research in International Business and Finance*, 70, Part A, 102301, 2024. https://doi.org/10.1016/j.ribaf.2024.102301

[CRO 14] CRO Forum, "Cyber resilience: The cyber risk challenge and the role of insurance", *CRO Forum*, 2014.

[CRO 23] CRO Forum, "Ransomware Threats, Countermeasures and Trends within the Insurance Industry: A CRO Forum White Paper", *CRO Forum*, 2023.

[CRU 15] CRUZ, M.G., PETERS, G.W., SHEVCHENKO, P.V., *Fundamental aspects of operational risk and insurance analytics: A handbook of operational risk.* John Wiley & Sons, Hoboken, New Jersey, 2015.

[DAM 07] D'AMICO, V., "Master the three phases of business continuity planning", *Business Strategy Series*, Vol. 8, 3, p. 214-220, 2007. DOI 10.1108/17515630710684213

[DUT 14] DUTTA, K., BABBEL, D., "Scenario Analysis in the Measurement of Operational Risk Capital: A Change of Measure Approach", *Journal of Risk and Insurance*, 81(2), p. 303–334, 2014. Retrieved from http://www.jstor.org/stable/24546806

[EC 24a] EUROPEAN COMMISSION, Commission Delegated Regulation (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers, European Commission, 2024.

[EC 24b] EUROPEAN COMMISSION, Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework, European Commission, 2024.

[EC 24c] EUROPEAN COMMISSION, Commission implementing Regulation (EU) 2024/2956 of 29 November 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to standard templates for the register of information, European Commission, 2024.

[EC 24d] EUROPEAN COMMISSION, Commission Delegated Regulation (EU) of 22.2.2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by specifying the criteria for the designation of ICT third-party service providers as critical for financial entities, European Commission, 2024.

[EGA 19] EGAN., R., CARTAGENA, S., MOHAMED, R., GOSRANI, V., GREWAL, J., ACHARYYA, M., DEE, A., BAJAJ, R., JAEGER, V.-J., KATZ, D., MEGHEN, P., SILLEY, M., NASSER-PROBERT, S., PIKINSKA, J., RUBIN, R., ANG, K., "Cyber operational risk scenarios for insurance companies", *British Actuarial Journal*, Vol. 24, p. 1-34, 2019. doi:10.1017/S1357321718000284

[EIOPA 20a] EIOPA, "Final Report on public consultation No. 19/270 on Guidelines on outsourcing to cloud service providers", 31 October 2020, EIOPA-BoS-20-002, European Insurance and Occupational Pensions Authority, 2020A.

[EIOPA 20b] EIOPA, "Guidelines on information and communication technology security and governance", EIOPA-BoS-20-600, European Insurance and Occupational Pensions Authority, 2020B.

[EIOPA 24] EIOPA, "Detailed account and EIOPA opinion on the impact of increased size thresholds as part of the Solvency II review on insurance undertakings in scope of DORA", 14 November 2024, EIOPA-BoS-24/425, European Insurance and Occupational Pensions Authority, 2024.

[EIOPA 25a] EIOPA, "Rulebook", EIOPA Rulebook: Solvency II Single Rulebook, European Insurance and Occupational Pensions Authority, 2025. https://www.eiopa.europa.eu/rulebook/solvency-ii-single-rulebook_en

[EIOPA 25b] EIOPA, "Digital Operational Resilience Act (DORA)", European Insurance and Occupational Pensions Authority, 2025. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[ELI 16] ELING, M., SCHNELL, W., "What do we know about cyber risk and cyber risk insurance?", *The Journal of Risk Finance*, Vol. 17, N. 5, p. 474-491, 2016. https://doi.org/10.1108/JRF-09-2016-0122

[ELI 18] ELING, M., LEHMANN, M., "The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks", *The Geneva Papers*, Vol. 43, p. 259-396, 2018. https://doi.org/10.1057/s41288-017-0073-0

[EP 22] EP. Regulations (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, European Parliament, L333/1, 2022.

[EPS 14] EPSTEIN, B., KHAN, D.C., "Application impact analysis: A risk-based approach to business continuity and disaster recovery", *Journal of Business Continuity & Emergency Planning*, Vol. 7, No. 3, p. 230-237, 2014.

[ESA 24] ESA, "Key findings from the 2024 ESAs Dry Run exercise", 17 December 2024, ESA 2024 35, European Banking Authority, European Insurance and Occupational Pensions Authority, European Securities and Markets Authority, 2024.

[FCA 19] FCA, "Building operational resilience: impact tolerances for important business services and feedback to DP18/04", December 2019, Consultation Paper CP19/32, Financial Conduct Authority, 2019.

[FCA 21a] FCA, "Building operational resilience: Feedback to CP19/32 and final rules", March 2021, Policy Statement PS21/3, Financial Conduct Authority, 2021.

[FCA 21b] FCA, "Operational Resilience Instrument 2021", FCA 2021/14, Financial Conduct Authority, 2021.

[FCA 25] FCA, "FCA Handbook", Financial Conduct Authority, 2025.

[FER 12] FERRIS, S., "Expensive Mistakes: Operational Risk in Life Insurance", *Risk Management and Insurance Review*, Vol. 15, No. 2, p. 263-288, 2012. DOI: 10.1111/j.1540-6296.2012.01221.x

[GAT 14] GATZERT, N., KOLB, A., "Risk Measurement and Management of Operational Risk in Insurance Companies from an Enterprise Perspective", *Journal of Risk and Insurance*, Vol. 81, No. 3, p. 683-708, 2014. DOID: 10.1111/j.1539-6975.2013.01519.x

[GER 24] GERKEN, C., KHAN, S., "Insurance Supervision: 2024 priorities", 11 January 2024, Dear [Chief Executive Officer], Prudential Regulation Authority, Bank of England, 2024.

[GIR 13] Girling, P., *Operational risk management: a complete guide to a successful operational risk framework*. Wiley, Hoboken, New Jersey, 2013.

[GOO 98] GOODHART, C., HARTMANN, P., LLEWELLYN, D, ROJAS-SUAREZ, L., WEISBROD, S., *Financial Regulation: Why, how and where now?* Routledge, London, 1998.

[GRI 21] GRIMA, S., KIZILKAYA, M., SOOD, K., DELICE, M.E., "The Perceived Effectiveness of Blockchain for Digital Operational Risk Resilience in the European Union Insurance Market Sector", *Journal of Risk and Financial Management*, 14, 363, 2021. https://doi.org/10.3390/jrfm14080363

[IAIS 16] IAIS, "Issues Paper on Cyber Risk to the Insurance Sector," August 2016, International Association of Insurance Supervisors, 2016.

[IAIS 18] IAIS, “Application Paper on Supervision of Insurer Cybersecurity”, November 2018, International Association of Insurance Supervisors, 2018.

[IAIS 23] IAIS, “Issues Paper on Insurance Sector Operational Resilience”, May 2023, International Association of Insurance Supervisors, 2023.

[IAIS 24a] IAIS, “Draft Application Paper on Operational Resilience Objectives [and Toolkit]”, 8 August 2024, International Association of Insurance Supervisors, 2024.

[IAIS 24b] IAIS, “Insurance Core Principles and Common Framework for the Supervision of Internationally Active Insurance Groups”, December 2024, International Association of Insurance Supervisors, 2024.

[INS 24A] INSURANCEEUROPE, “Insurance Europe response to the second batch of draft DORA Level 2 measures”, 4 March 2024, EXCO-CS-24-012, Insurance Europe, 2024.

[INS 24b] INSURANCEEUROPE, “Digital Transformation”, June 2024, Insurance Matters, Insurance Europe, 2024.

[INS 25] INSURANCEEUROPE, “ Cyber: Insurers’ key role in increasing cyber resilience ”, Insurance Europe, 2025. https://www.insuranceeurope.eu/priorities/27/cyber

[LL] LLOYD’S OF LONDON, “What is Operational Resilience?” Lloyd’s of London [undated].

[LL 23] LLOYD’S OF LONDON, “Market Operational Resilience Framework”, August 2023, Lloyd’s of London, 2023.

[LL 24a] LLOYD’S OF LONDON, “Operational Resilience Self-Assessments: Trends & Observations Report”, September 2024, Lloyd’s of London, 2024A.

[LL 24b] LLOYD’S OF LONDON, “Principles for doing business at Lloyd’s”, November 2024, Lloyd’s of London, 2024B.

[LL 24c] LLOYD’S OF LONDON, “Principles for doing business at Lloyd’s: Summary of revisions”, November 2024, Lloyd’s of London, 2024C.

[LL 25] LLOYD’S OF LONDON, “Principle 12: Operational Resilience”, Lloyd’s of London, 2025. https://www.lloyds.com/conducting-business/market-oversight/principles-for-doing-business-at-lloyds/operational-resilience

[LMA 20] LMA, “Joint Lloyd’s/LMA response to PRA consultation on Building Operational Resilience”, 30 September 2020, Lloyd’s Market Association, 2020.

[LMA 21a] LMA, “LMA Operational Resilience Guidance”, 29 April 2021, LMA Operational Resilience Working Group, Lloyd’s Market Association, 2021.

[LMA 21b] LMA, “IBS Selection Criteria and Scoring”, July 2021, LMA Operational Resilience Working Group, Lloyd’s Market Association, 2021.

[LMA 22a] LMA, “Operational Resilience Benchmarking Survey #4”, January 2022, Lloyd’s Market Association, 2022.

[LMA 22b] LMA, “LMA response to DP3/22 – Operational resilience: Critical third parties to the UK financial sector”, 16 December 2022, Lloyd’s Market Association, 2022.

[LMA 25] LMA, “Operational Resilience”, Lloyd’s Market Association, 2025. https://www.lmalloyds.com/LMA/Market_Processes/Operational_Resilience_home.aspx

[MCS 18] MCSHANE, M., “Enterprise risk management: history and a design science proposal”, *Journal of Risk Finance*, Vol. 19, No. 2, p. 137-153, 2018. https://doi.org/10.1108/JRF-03-2017-0048

[MIL 24] MILLS, S., “Building operational resilience at the heart of the financial system”, Speech by Sasha Mills Given at the London Institute of Banking and Finance, Bank of England, 2024.

[NAI 19] NAIM, P., CONDAMIN, L., *Operational Risk Modeling in Financial Services: The Exposure, Occurrence, Impact Method*. John Wiley & Sons, Chichester, West Sussex, 2019.

[NEL 18] NELSON, L., “Resilience and continuity in an interconnected and changing world”, Speech by Lyndon Nelson, given at the 20th Annual Operational Risk Europe conference, London, Bank of England, 2018.

[NIE 19] NIEMIMAA, M., JARVELAINEN, J., HEIKKILA, M., HEIKKILA, J., “Business continuity of business models: Evaluating the resilience of business models for contingencies”, *International Journal of Information Management*, Vol. 49, p. 208–216, 2019. https://doi.org/10.1016/j.ijinfomgt.2019.04.010

[ORCG 20] ORCG, “Scenarios and Scenario Testing Industry Guidance”, Operational Resilience Collaboration Group. August 2020.

[PET 11] PETERS, G.W., BYRNES, A.D., SHEVCHENKO, P.V., "Impact of insurance for operational risk: Is it worthwhile to insure or be insured for severe losses?", *Insurance: Mathematics and Economics*, Vol. 48, Issue 2, p. 287-303, 2011. https://doi.org/10.1016/j.insmatheco.2010.12.001

[PRA 21a] PRA, "Operational resilience: Impact tolerances for important business services", March 2021, Policy Statement, PS6/21, Prudential Regulation Authority, Bank of England, 2021A.

[PRA 21b] PRA, "Outsourcing and third party risk management", March 2021, Policy Statement, PS7/21, Prudential Regulation Authority, Bank of England, 2021B.

[PRA 22] PRA, "Operational resilience: Impact tolerances for important business services", March 2022, Updating March 2021, Supervisory Statement SS1/21, Prudential Regulation Authority, Bank of England, 2022.

[PRA 23] PRA, "The Prudential Regulation Authority's approach to insurance supervision", July 2023, Prudential Regulation Authority, Bank of England, 2023.

[PRA 24a] PRA, "Operational resilience", November 2024, Updating March 2021, Statement of Policy, Prudential Regulation Authority, Bank of England, 2024.

[PRA 24b] PRA, "Outsourcing and third party risk management", November 2024, updating March 2021, Supervisory Statement SS2/21, Prudential Regulation Authority, 2024.

[PRA 25] PRA, "The PRA Rulebook", Prudential Regulation Authority, 2025.

[SAE 23] SAEED, S., ALTAMIMI, S.A., ALKAYYAL, N.A., ALSHEHRI, E., ALABBAD, D.A., "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations", *Sensors*, 23, 6666, 2023. https://doi.org/10.3390/s23156666

[SAH 15] SAHEBJAMNIA, N., TORABI, S.A., MANSOURI, S.A., "Innovative Applications of O.R. Integrated business continuity and disaster recovery planning: Towards organizational resilience", *European Journal of Operational Research*, Vol. 242, Issue 1, p. 261-273, 2015. http://dx.doi.org/10.1016/j.ejor.2014.09.055

[SAH 18] SAHEBJAMNIA, N., TORABI, S.A., MANSOURI, S.A., "Building organizational resilience in the face of multiple disruptions", *International Journal of Production Economics*, Vol. 197, p. 63-83, 2018. https://doi.org/10.1016/j.ijpe.2017.12.009

[STH 23] STHEEMAN, E., "Cyber risks and operational resilience: getting prepared", Speech by Elisabeth Stheeman, given at the London School of Economics, Bank of England, 2023.

[TRU 25] TRURAN, G., KHAN, S., "Insurance Supervision: 2025 priorities", 9 January 2025, Dear [Chief Executive Officer], Prudential Regulation Authority, Bank of England, 2025.

[TUC 15] TUCKER, E., *Business continuity from preparedness to recovery: a standards-based approach*, Butterworth-Heinemann, Elsevier, London, 2015.

[VAN 06] Van Grinsven, J.H.M., *Improving Operational Risk Management*, 2nd Edition, Sage Publications, IOS Press, Amsterdam, The Netherlands, 2006.

[VYS 20] VYSKOČIL, M., "Scenario Analysis Approach for Operational Risk in Insurance Companies", *Economic Studies and Analyses*, University of Finance and Administration, ACTA VŠFS, 2/2020, Vol. 14, p. 153-165, 2020. http://dx.doi.org/10.37355/acta-2020/2-05

[WIB 13] WIBOONRATR, M., KOSAVISUTTE, K., "Optimal strategic decision for disaster recovery", *International Journal of Management Science and Engineering Management*, Vol. 4, No. 4, p. 260-269, 2013. https://doi.org/10.1080/17509653.2009.10671079

[ZHA 23] ZHANG, H., LI, E.Y., JIANG, J., FU, W., PENG, S., ZHAN, S., "Resilience of Operational Performance in China's Insurance Companies: A Dynamic Data Envelopment Analysis", *IEEE Access*, Vol. 11, 2023. DOI: 10.1109/ACCESS.2023.3323587

[ZHI 17] ZHING, Z., ZIO, E., "An integrated modeling framework for quantitative business continuity assessment", *Process Safety and Environmental Protection*. Vol. 106, p. 76-88, 2017. http://dx.doi.org/10.1016/j.psep.2016.12.002

